The United States Department of the Treasury

TERRORIST FINANCE TRACKING PROGRAM

Questions and Answers

After the terrorist attacks on September 11, 2001, the United States Department of the Treasury initiated the Terrorist Finance Tracking Program (TFTP) to identify, track, and pursue terrorists – such as Al-Qaida – and their networks. Since that time, the TFTP has provided valuable leads – more than 1,550 of them provided to European Union (EU) Member States – that have aided in the prevention or investigation of many of the most visible and violent terrorist attacks and attempted attacks of the past decade.

The European Commission and the United States (US) have concluded negotiations toward a new agreement between the EU and the US on the transfer and processing of data for purposes of the TFTP. This document is intended to answer many of the most common questions about the TFTP and the new Agreement.

Q.1: What are the changes in the new Agreement from the earlier interim Agreement?

A.1: There are at least a dozen significant changes in the new Agreement, including:

1. A new article outlining a right of access, including a procedure to verify that individual data protection rights have been respected and with specified roles for European data protection authorities and the US Treasury Department's privacy officer;
2. A new article outlining a right to rectification, erasure, or blocking of data, with specified roles for European data protection authorities and the US Treasury Department's privacy officer;
3. A new article on transparency, requiring the US Treasury Department to post specified information about the TFTP on its website and to provide contact information for persons with questions;
4. An expanded article on redress which provides for equal treatment by the US Treasury Department to all persons in the application of its administrative processes, regardless of nationality or place of residence, as well as a clause that outlines the non-discriminatory avenues of judicial redress the US provides;
5. An expanded article on data safeguards to ensure data security and integrity and necessary and proportionate processing of data, as well as a new clause recognizing the principle of proportionality that guides the Agreement;
6. A new article on monitoring of safeguards and controls, including new oversight roles for an EU-appointed real-time independent overseer and the US Treasury Department's Inspector General;
7. A new article providing that the European Commission will carry out a study into the possibility of a future EU system similar to the TFTP and pledging US support for such a system;
8. A new article limiting the transfer of information to third countries;
9. A new article regarding the maintaining of the accuracy of the information;
10. A new article governing the retention of data, with additional requirements on the US and an obligation for the US and the EU to prepare a report on the value of data retained for multiple years;
11. A new mechanism to compel the data, ensuring EU review of all US data requests (via Europol) and eliminating the mutual legal assistance treaty (MLAT) approach; and
12. An expanded joint EU-US review provision, including review teams comprised of experts in security and data protection, as well as a person

with judicial experience, a greater number of items to be reviewed, and the provision of a report to the European Parliament and the Council.

Q.2: What is the value of the TFTP?

A.2: Since its inception in 2001, the TFTP has provided valuable lead information that has aided in the prevention of many terrorist attacks and in the investigation of many of the most visible and violent terrorist attacks and attempted attacks of the past decade, including, for example:

- the Bali bombings in 2002;
- the Madrid train bombings in 2004;
- the Van Gogh terrorist-related murder in the Netherlands in 2004;
- the bombings in London in 2005;
- the liquid bomb plot against transatlantic aircraft in 2006;
- the plan to attack New York's John F. Kennedy airport in 2007;
- the Islamic Jihad Union plot to attack sites in Germany in 2007;
- the attacks in Mumbai in 2008; and
- the Jakarta hotel attacks in 2009.

A significant number of the leads generated by the TFTP have been shared with EU Member State Governments, with more than 1,550 such reports shared to date. An independent person appointed by the EU to examine the TFTP reported in 2008 and in early 2010 that TFTP leads shared with EU authorities had not only been extremely valuable in investigating terrorist attacks which have taken place in Europe over the last eight years, but had also been instrumental in preventing a number of terrorist attacks in Europe and elsewhere.

Q.3: How does the TFTP operate?

A.3: Under the TFTP, the US Treasury Department issues administrative production orders (Requests) to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an international bank-to-bank clearinghouse, for narrow sets of financial messaging data transmitted between financial institutions which are relevant to terrorism investigations. Requests are narrowly tailored based on past analyses of relevant message types, geography, and perceived terrorism threats. The subsets of data transferred to the US Treasury Department pursuant to the Requests are subject to strict security measures and cannot be searched except where various elaborate safeguards (detailed below) are satisfied.

Under the new Agreement, the US Treasury Department will provide a copy of any Request for data stored in Europe, along with any

supplemental documents, to Europol to verify whether the Request clearly identifies the data requested, is narrowly tailored, and substantiates the necessity of the data. Once that verification has occurred, Europol will so notify the data provider, and the data provider will transmit the data to the US Treasury Department.

Q.4: What are the safeguards protecting the data?

A.4: President Obama has made the protection of privacy and civil liberties a top priority. Consistent with this decision, the US Treasury Department has agreed to apply extraordinarily strict controls – including a series of new measures – over the data to ensure data security and integrity, as well as necessary and proportionate processing of data. Reports issued in 2008 and early 2010 by an independent person appointed by the EU concluded that the US had satisfied all data protection safeguards. These safeguards include the following:

- TFTP data are maintained in a physically secure, stand-alone computer network – not connected to any other data system – and subject to highly limited access rights.
- Data may be searched only for counter-terrorism purposes and not for any other type of criminal activity or for any other purpose, including counter-proliferation.
- No search may be conducted on data unless a TFTP investigator provides pre-existing information demonstrating a nexus between the subject of the search and terrorism or its financing.
- The TFTP may not be used for data mining or any other type of algorithmic or automated profiling or computer filtering.
- Detailed logs are maintained of all searches made, including the identity of the investigator performing the search, date and time of the search, search terms used, and justification for the search.
- A select group of independent overseers with security clearances – not employed by or affiliated with the US Government – have access to all searches of the provided data undertaken by a TFTP investigator, and can block any and all searches as they occur if they do not satisfy all of the safeguards.

In addition to the preceding safeguards, the new TFTP Agreement requires the following new and improved oversight measures with respect to the safeguards:

- The EU has the authority to appoint a person to serve as an independent overseer of TFTP searches of the provided data, with the authority to review searches in real-time and retrospectively and to query the searches.

- The Inspector General of the US Treasury Department also will ensure that the oversight and audit functions are performed pursuant to applicable audit standards.
- A team of EU and US security and data protection experts, as well as a person with judicial experience, shall jointly review the implementation, value, and safeguards of the TFTP on a regular basis, including after six months from the start of the Agreement, and the European Commission subsequently will present a report on the review to the European Parliament and the Council.

An external auditing firm appointed by the data provider continues to perform a separate, independent audit. The external auditors have full access to all TFTP systems and personnel.

Q.5: What redress provisions are available to EU citizens and residents?

A.5: Under the new Agreement, persons are provided the right to seek access to data, including a confirmation whether their data protection rights have been respected and whether any improper processing of their personal data has occurred, as well as the right to seek rectification, erasure, or blocking of any inaccurate data. Requests for data, confirmations, or rectification may be submitted to the relevant European national data protection authority, which shall transmit the requests to the privacy officer of the US Treasury Department. After an appropriate review, the privacy officer then must: (a) inform the relevant European national data protection authority whether personal data may be disclosed to the data subject or whether data have been rectified; (b) confirm whether the data subject's rights have been duly respected; and (c) where access to personal data is refused based on reasonable exemptions from disclosure or rectification is refused, explain the refusal in writing and provide information on the means available for seeking administrative and judicial redress in the United States.

The Agreement further provides that any person who considers his or her personal data to have been processed improperly may seek effective administrative or judicial redress in accordance with the laws of the EU, its Member States, and the US. The US Treasury Department has agreed to treat all persons equally in the application of its administrative processes, regardless of nationality or country of residence.

The US also agreed that all persons, regardless of nationality or country of residence, shall have available under US law a process for seeking judicial redress from an adverse administrative action. The Administrative Procedure Act, for example, allows any person who has suffered harm as a result of a US Government action to seek judicial review of that action. Other examples of relevant laws allowing non-discriminatory

judicial redress include the Computer Fraud and Abuse Act, which authorizes any person who suffers damage or loss by reason of a violation of the Act to maintain a civil action against the violator, including, as appropriate, a US government official, to obtain damages or other relief, and the Freedom of Information Act, which allows individuals to utilize administrative and judicial remedies to seek government information.

Q.6: How long are data stored under the TFTP?

A.6: The US has agreed to destroy data after five years, which is the same time period the EU uses under Directive 2005/60/EC (on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing) and Regulation (EC) No. 1781/2006 (on information on the payer accompanying transfers of funds). Leads generated for use in specific matters are retained for no longer than necessary for specific investigations or prosecutions for which they are used.

The new Agreement requires the EU and the US to prepare a joint report regarding the value of TFTP data, with particular emphasis on the value of data retained for multiple years. It also stipulates that the US, in sharing leads based on TFTP data with third countries, shall request that the information be deleted as soon as it is no longer necessary for the counter-terrorism purpose for which it was shared.

Q.7: Why can't ordinary law enforcement requests be used to gather this same information on suspected terrorists?

A.7: The primary reason why ordinary law enforcement requests would not be sufficient is the international nature of terrorism and the difficulties that global scope may cause investigators in any country or countries. We may have reliable evidence, for example, that a specific terrorist is sending money from Africa to Europe or elsewhere for an attack against bus stations, but we may not know the banks to which he or she is sending the money or even the countries in which those banks are located. It would be impossible for the US or any other country to issue law enforcement requests for the relevant records of every bank in every country in the EU or around the world. The TFTP allows investigators to conduct targeted searches to identify data from international bank-to-bank transfers, locating the source from which a terrorist's money is being sent and the place to where it is going, and to alert relevant governments of the information they may need to investigate further or disrupt terrorist activity.

Q.8: Why can't SWIFT conduct such searches itself?

A.8: SWIFT has said that it has no ability to search its data. Therefore, after the September 11 attacks, the US agreed to bear the resource and time cost to develop and implement the TFTP to conduct pinpoint searches of the data that might help to prevent or investigate attacks.

Q.9: I heard that the TFTP may be the reason my bank blocked a transaction to my account and my goods were stopped at a border crossing. Is that possible?

A.9: No. The TFTP cannot interdict or view "live" transactions as they occur; instead, it involves a narrow review of specific, terrorism-related financial transactions that already have occurred in order to further government investigations of terrorist plots and activity.

Q.10: Does the US send an EU customer's transaction data to countries outside of the EU?

A.10: For nearly 10 years, the US has shared leads generated by the TFTP with relevant Governments for counter-terrorism purposes only. We do this consistent with UN Security Council Resolution 1373 (2001) and its directives:

- that all States shall take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
- that States shall afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts;
- that States should find ways of intensifying and accelerating the exchange of operational information;
- that States should exchange information in accordance with international and domestic law; and
- that States should cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and to take action against perpetrators of such attacks.

The new Agreement limits the transfer to third countries of EU persons' data and authorizes such transfers only for counter-terrorism purposes and subject to a variety of additional safeguards.